PRB 01-7E

IN BRIEF

Parliamentary Research Branch
Library of Parliament

Michel Rossignol
28 June 2001

Critical Infrastructure Protection and Emergency Preparedness

INTRODUCTION

Computer technology is now such a pervasive element of modern society that its benefits for governments, corporations, public utilities, and many other organizations are taken for granted. However, the computer age has also introduced new vulnerabilities. The technology is so widespread and interconnected in the banking, commercial, energy, and manufacturing sectors that any deliberate or accidental interference can have costly repercussions. Furthermore, any tampering with the computers managing public utilities such as hydroelectric plants and related infrastructure such as dams could cause serious environmental damage as well as major disruptions in commercial transactions and industrial production. A country's critical infrastructure could be the target of attacks by terrorist groups based at home or abroad, by foreign governments, and by criminal elements. The widespread disruptions caused by some recent computer hacking incidents are perhaps only a small sample of the impact a concerted effort to paralyze the essential infrastructure of a country through its computer systems could have. In the not-so-distant future, the capacity to wage offensive as well as defensive information technology warfare could become an increasingly important element of a country's ability to ensure its security, but this raises complex moral and ethical issues which are just starting to be debated.

INCREASED EMPHASIS IN THE UNITED STATES

In the meantime, the potential impact of just a few isolated attacks on a country's essential infrastructure has raised concerns within government and military circles. The United States in particular has devoted considerable efforts and resources to bolster its ability to deal with such attacks. Indeed, in the late 1990s, the United States became increasingly conscious that despite its great military power, it could still be very vulnerable to what has been called asymmetrical threats. Instead of directly confronting the United States, military forces, states or groups antagonistic towards the U.S. could launch terrorist strikes against that country's critical infrastructure in order to damage the economy and terrorize the population. To increase the impact of their actions on the civil population, antagonistic states and groups could also resort to terrorist attacks using weapons of mass destruction (WMD) including small nuclear bombs and chemical and biological agents. Thus, in conjunction with measures taken to protect its vital computer systems, the U.S. has also improved its capacity to deal with the consequences of terrorist attacks with weapons of mass destruction.

Given the emphasis on the protection of the population and the infrastructure within the continental United States, the measures taken by the U.S. government to counter asymmetrical threats are often grouped within what is called homeland defence. The key elements of homeland defence include two Presidential Decision Directives of 1998: PDD-62, which was aimed at increasing the capacity of civilian police and medical officials as well as some military units to deal with the consequences of WMD attacks; and PDD-63, which sought to improve the coordination of the various agencies involved in protecting information technology systems. These agencies include: the National Infrastructure Protection Centre (NIPC), within the Federal Bureau of Investigation (FBI), which is the focal point for threat assessment, warning, investigation, and response to threats to or attacks against the critical infrastructure; and the Critical Infrastructure Assurance Office (CIAO), housed within the Commerce Department, which is involved in the coordination of U.S. Government initiatives. The U.S. Space Command was designated as the lead organization for the protection of military computer systems. The complex inter-agency process involved in dealing with cyber-related issues was described in

the National Plan for Information Systems Protection issued by the U.S. Government in January 2000. The new Bush Administration also gives a high priority to critical infrastructure protection, but has announced its intention of producing a new version of the National Plan by late 2001.

Critical infrastructure protection is inevitably complex because it involves privately owned elements as well as government and military ones. Indeed, government and military systems represent a relatively small portion of the U.S. critical infrastructure when compared to the extensive privately owned and operated systems in the banking, commercial, and public utilities sectors. Thus, part of the efforts deployed by the U.S. Government to protect the infrastructure involves close cooperation with the private sector in order to: raise awareness of the issues; and improve coordination – between corporations and government agencies – of measures to deal with cyber attacks. However, the interconnection between computer systems does not end at borders, and the cooperation of other countries is also crucial in critical infrastructure protection.

CANADIAN INITIATIVES

Indeed, as already demonstrated on numerous occasions, hacking and other types of cyber attacks against U.S. systems can have serious repercussions for the critical infrastructure of many other countries. Banking, commercial, and government systems throughout the world are so interrelated that few countries can afford to neglect preparations to deal with the consequences of deliberate or accidental interference. Thus, in February 2001, Prime Minister Jean Chrétien announced the establishment within the Department of National Defence of the Office of Critical Infrastructure Protection and Emergency Preparedness (OCIPEP) which has the task of developing and implementing a comprehensive approach to the protection of Canada's critical infrastructure. The new agency encompasses the functions of what used to be called Emergency Preparedness Canada since it may have to deal with the consequences of disruptions in computer systems monitoring or the operation of physical elements of the critical infrastructure such as hydroelectric dams and oil pipelines. The emergency preparedness side of the agency will also continue to prepare for, and respond to, natural disasters and other situations unrelated to cyber attacks as Emergency Preparedness Canada did in the past. Indeed, a high level of preparedness will no doubt have to be maintained if only because of the possible increase in the number of extreme weather events due to climate change. However, the creation of a new agency is also aimed at bringing Canada's critical infrastructure protection up to speed in light of developments in the U.S. and in other countries. In terms of cyber attacks, Canada does not necessarily face as great a threat as the U.S. which is the main target of a number of antagonistic states around the world. However, Canada cannot afford to lag too far behind its allies in the protection of its critical infrastructure because there is always a possibility that terrorist groups could launch attacks against the U.S. through Canada. Besides, Canada might suffer collateral damage as a result of cyber or WMD attacks within the U.S., regardless of the route chosen by antagonistic states and groups to carry out their aggression.

Nevertheless, despite the creation of OCIPEP, the Solicitor General remains the lead minister for public safety in Canada. Indeed, as the minister responsible for OCIPEP, the Minister of National Defence will collaborate closely with the Solicitor General and other ministers to ensure a coherent and comprehensive national approach to critical infrastructure protection and emergency preparedness. Thus, the new office will not take over or coordinate the work of the Canadian Security Intelligence Service (CSIS) and the R.C.M.P. in assessing and dealing with the terrorist threat. It will instead cooperate with them and rely on their assessments of potential threats, as pointed out by Margaret Purdy, the Associate Deputy Minister of National Defence, who is responsible for OCIPEP within the department, during the 29 May 2001 meeting of the Standing Committee on National Defence and Veterans Affairs of the House of Commons. The office will also benefit from the ongoing work of organizations within the Department of National Defence involved in the protection of military and government computer systems. One of these organizations is the Communications Security Establishment (CSE) which advises government departments on network security by providing, for example, threat risk assessment support services.

However, as in the U.S., ensuring the security of military and federal government information technology systems is only one element of critical infrastructure protection. After all, as the Minister of National Defence pointed out in a 26 June 2001 speech during the World Conference on Disaster Management held in Hamilton, Ontario, only about 10% of Canada's critical infrastructure is owned or operated by the federal government. Although private

infrastructure owners and operators have developed their own information technology security programs, considerable work remains to be done to improve cooperation such as information-sharing between the public and the private elements of Canada's critical infrastructure. Thus, as part of its development of a National Framework for critical infrastructure protection, OCIPEP will not only work to improve the federal government's capacity to protect its information technology systems, but also develop partnerships with private infrastructure owners and operators and with business organizations such as the Canadian Chamber of Commerce and the Canadian Bankers Association. However, even if the protection of Canada's information technology systems against intentional disruptions is maintained at a high level, the country may still have to deal with major natural disasters and cannot afford to be complacent about emergency preparedness. Thus, on 26 June 2001, the Minister of National Defence also announced that the Government of Canada will begin consultations, led by OCIPEP, with the provinces and the territories and with the private sector in order to develop a National Disaster Mitigation Strategy aimed at saving lives and reducing the impact of disasters.

Indeed, the efforts deployed to protect information technology systems and to bolster emergency preparedness are in keeping with the growing recognition over the years that a country's security depends on more than its ability to defend itself against attacks by foreign military forces. In the absence of a sufficient capacity to counter the terrorist threat and to mitigate the effects of major natural disasters, a country could face serious social and economic disruptions which could seriously undermine its security. Thus, the protection of the critical infrastructure will likely continue to be a major preoccupation of the Canadian government for some time to come, especially because considerable work remains to be done in the development of closer cooperation between the public and private sectors.

EN BREF

Direction de la recherche parlementaire
Bibliothèque du Parlement

Michel Rossignol
Le 28 juin 2001

Protection des infrastructures essentielles et protection civile

INTRODUCTION

Les ordinateurs sont aujourd'hui tellement répandus dans notre société moderne que nous tenons pour acquis les avantages qu'ils procurent aux gouvernements, aux entreprises aux services publics et à beaucoup d'autres organisations. Mais l'ère informatique a aussi ses points faibles. La technologie informatique est à ce point omniprésente et comporte des liens si étroits dans les secteurs des banques, du commerce, de l'énergie et de la fabrication que toute perturbation délibérée ou accidentelle à cet égard risquerait d'avoir des répercussions coûteuses. En outre, toute altération des ordinateurs servant à la gestion des systèmes des services publics – par exemple les usines hydroélectriques et les installations connexes comme les barrages – pourrait causer de graves dommages à l'environnement, ainsi que d'importants dérèglements dans les transactions commerciales et la production industrielle. L'infrastructure essentielle d'un pays pourrait être la cible d'attaques de groupes terroristes basés dans ce pays même ou à l'étranger, ou encore de gouvernements étrangers ou d'éléments criminels. Les perturbations majeures attribuables à certains incidents de piraterie informatique récents pourraient bien n'être qu'un petit échantillon des retombées que pourrait avoir un effort concerté pour paralyser l'infrastructure essentielle d'un pays en s'attaquant à ses systèmes informatiques. Dans un avenir relativement rapproché, la possibilité de lancer des opérations tant offensives que défensives dans le domaine de la technologie informatique pourrait devenir un élément de plus en plus important de la capacité des pays à assurer leur sécurité, mais cette perspective soulève des questions morales complexes dont nous commençons tout juste à débattre.

INTÉRÊT ACCRU DES ÉTATS-UNIS

Les cercles gouvernementaux et militaires se préoccupent cependant déjà des répercussions que pourraient avoir une poignée d'attaques isolées visant l'infrastructure essentielle d'un pays. Les États-Unis, en particulier, ont consacré des efforts et des ressources considérables à diverses mesures visant à renforcer leur capacité de faire face à des attaques de ce genre. En effet, à la fin des années 90, les Américains ont pris conscience du fait que, malgré toute leur puissance militaire, ils demeuraient très vulnérables à ce qu'on a appelé les menaces asymétriques. Plutôt que d'affronter directement les forces armées américaines, des États ou des groupes hostiles aux États-Unis pourraient lancer des attaques terroristes contre l'infrastructure essentielle de ce pays afin de ralentir son économie et de terroriser sa population. Pour que leurs actes aient encore plus d'effets sur les populations civiles, ces États et groupes hostiles pourraient également lancer des attaques terroristes à l'aide d'armes de destruction massive (ADM) comme de petites bombes nucléaires, ou encore des agents chimiques ou biologiques. C'est pourquoi, parallèlement aux mesures prises pour protéger leurs systèmes informatiques essentiels, les Américains ont également renforcé leur capacité de faire face aux conséquences d'attaques terroristes perpétrées à l'aide d'armes de destruction massive.

Étant donné l'importance accordée à la protection de la population et de l'infrastructure sur le territoire des États-Unis, les mesures prises par le gouvernement américain pour contrer ces menaces asymétriques sont souvent associées à ce qu'on appelle la défense intérieure. Celle-ci s'articule surtout autour de deux directives présidentielles datant de 1998, la PDD-62, qui visait à fournir à la police civile, aux médecins et à certaines unités militaires de meilleurs moyens pour faire face aux conséquences de l'utilisation d'ADM, et la PDD-63, qui avait pour but d'améliorer la

coordination des divers organismes s'occupant de la protection des systèmes de technologie de l'information. Il s'agit notamment du National Infrastructure Protection Centre (NIPC) – qui relève du Federal Bureau of Investigation (FBI) et qui est le point central de tout ce qui touche l'évaluation de la menace, les mises en garde, les enquêtes et les réactions à la menace ou aux attaques contre l'infrastructure essentielle – et du Critical Infrastructure Assurance Office (CIAO) – qui fait partie du département du Commerce et qui coordonne les initiatives du gouvernement américain. Le U.S. Space Command a été chargé pour sa part d'orchestrer les mesures de protection des systèmes informatiques militaires. Le processus complexe de collaboration entre organismes dans le domaine des systèmes informatiques est décrit dans le plan national pour la protection des systèmes de technologie de l'information que le gouvernement américain a rendu public en janvier 2000. La nouvelle administration Bush accorde elle aussi une grande importance à la protection de l'infrastructure essentielle, et elle a annoncé son intention de produire une nouvelle version de ce plan national d'ici la fin de 2001.

La protection de l'infrastructure essentielle est nécessairement complexe parce qu'elle englobe non seulement des éléments gouvernementaux et militaires, mais également des intérêts privés. En fait, les systèmes gouvernementaux et militaires ne représentent qu'une portion relativement minime de l'infrastructure essentielle des États-Unis, comparativement aux nombreux systèmes appartenant à des intérêts privés, et exploités par eux, dans les secteurs des banques, du commerce et des services publics. Une partie des efforts déployés par le gouvernement américain pour protéger cette infrastructure nécessite par conséquent une étroite collaboration avec le secteur privé, dans le but de faire prendre conscience des enjeux et d'améliorer la coordination des mesures visant à contrer la menace de cyberattaques dans les entreprises et les organismes gouvernementaux. Cependant, l'interconnexion des systèmes informatiques ne prend pas fin aux frontières, et la coopération des autres pays est également indispensable à la protection de l'infrastructure essentielle.

LES INITIATIVES CANADIENNES

D'ailleurs, comme nous l'avons déjà vu à maintes reprises, la piraterie informatique et les autres types de cyberattaques contre des systèmes américains peuvent avoir de graves répercussions sur l'infrastructure essentielle de nombreux autres pays. Les systèmes bancaires, commerciaux et gouvernementaux du monde entier étant étroitement liés, rares sont les pays qui peuvent se permettre de négliger les préparatifs nécessaires pour réagir aux conséquences de perturbations délibérées ou accidentelles dans ce domaine. C'est ainsi que le premier ministre Jean Chrétien a annoncé en février 2001 la création, à l'intérieur du ministère de la Défense nationale, du Bureau de la protection des infrastructures essentielles et de la protection civile (BPIEPC), chargé d'élaborer et de mettre en oeuvre une politique globale de protection de l'infrastructure essentielle du Canada. Ce nouvel organisme a hérité des fonctions qu'assumait anciennement Protection civile Canada, puisqu'il pourrait avoir à s'occuper des conséquences de perturbations dans la surveillance des systèmes informatiques ou dans l'exploitation des éléments physiques de l'infrastructure essentielle, par exemple les barrages hydroélectriques et les oléoducs. Ses services de protection civile devront également poursuivre des activités de planification et d'intervention en cas de catastrophes naturelles et d'autres situations qui n'auraient rien à voir avec des cyberattaques, comme le faisait Protection civile Canada dans le passé. De fait, il faudra sans aucun doute maintenir un haut niveau de préparation, ne serait-ce qu'à cause de l'augmentation possible du nombre de crises météorologiques attribuables aux changements climatiques. Cependant, la création de ce nouvel organisme vise également à renforcer la protection de l'infrastructure essentielle du Canada à la lumière de ce qui se fait aux États-Unis et dans d'autres pays. L'éventualité de cyberattaques ne représente peut-être pas une menace aussi grave pour le Canada que pour les États-Unis, qui constituent la principale cible d'un certain nombre d'États hostiles à travers le monde. Le Canada ne peut cependant pas se permettre de prendre trop de retard sur ses alliés, pour la protection de son infrastructure essentielle, puisqu'il est toujours possible que des groupes terroristes lancent depuis le Canada des attaques terroristes contre les États-Unis. En outre, le Canada pourrait subir des dommages collatéraux résultant d'attaques perpétrées contre les États-Unis par des moyens informatiques ou à l'aide d'ADM, quelle que soit la voie choisie pour ce faire par les États et groupes qui leur sont hostiles.

Néanmoins, et malgré la création du BPIEPC, le Solliciteur général demeure le principal ministre chargé de la sécurité publique au Canada. En fait, en tant que ministre responsable du BPIEPC, le ministre de la Défense nationale travaillera en étroite

collaboration avec lui, ainsi qu'avec d'autres ministres, pour assurer la mise en oeuvre d'une approche nationale cohérente et globale pour la protection de l'infrastructure essentielle et la protection civile. Le nouvel organisme ne sera donc pas chargé d'effectuer ou de coordonner le travail du Service canadien du renseignement de sécurité (SCRS) et de la GRC en ce qui concerne l'évaluation de la menace terroriste et les mesures à prendre pour y répondre. Il collaborera plutôt avec eux et se fondera sur leurs évaluations de la menace potentielle, comme l'a indiqué Margaret Purdy, la sous-ministre déléguée de la Défense nationale qui est responsable du BPIEPC au sein du Ministère, lors de sa comparution devant le Comité permanent de la défense nationale et des anciens combattants de la Chambre des communes le 29 mai 2001. Le Bureau bénéficiera également du travail courant des organisations chargées de la protection des systèmes informatiques militaires et gouvernementaux au ministère de la Défense nationale. Il s'agit notamment du Centre de la sécurité des télécommunications (CST), qui conseille les ministères sur la sécurité des réseaux en fournissant par exemple des services de soutien en matière d'évaluation du risque.

Cependant, comme aux États-Unis, la sécurité des systèmes informatiques militaires et de ceux du gouvernement fédéral n'est qu'un élément de la protection de l'infrastructure essentielle. Après tout, comme l'a fait remarquer le ministre de la Défense nationale dans le discours qu'il a prononcé le 26 juin 2001 à l'occasion de la Conférence mondiale sur la gestion des opérations en cas de catastrophe qui s'est tenue à Hamilton (Ontario), le gouvernement fédéral ne possède et n'exploite qu'environ 10 p. 100 de l'infrastructure essentielle du pays. Bien que les propriétaires et exploitants privés aient mis au point leurs propres programmes de sécurité en matière de technologie de l'information, il reste énormément de travail à faire pour améliorer la coopération à ce chapitre, par exemple les échanges d'information entre les responsables publics et privés de l'infrastructure essentielle du Canada. Par conséquent, dans ses efforts pour élaborer un cadre national de protection de l'infrastructure essentielle, le BPIEPC cherchera non seulement à améliorer la protection des systèmes informatiques du gouvernement fédéral, mais également à mettre en place des partenariats avec les propriétaires et exploitants privés et avec les organisations d'affaires comme la Chambre de commerce du Canada et l'Association des banquiers canadiens. Toutefois, même si la protection des systèmes informatiques canadiens contre les perturbations intentionnelles est maintenue à un haut niveau, le pays pourrait toujours avoir à faire face à des catastrophes naturelles majeures; il ne peut donc pas se permettre de négliger sa planification d'urgence. C'est pourquoi le ministre de la Défense nationale a aussi annoncé, le 26 juin 2001, que le gouvernement du Canada entreprendra, sous la direction du BPIEPC, des consultations avec les provinces et territoires et avec le secteur privé afin d'établir une stratégie nationale d'atténuation des catastrophes visant à sauver des vies et à limiter les conséquences des catastrophes.

En fait, les efforts déployés pour protéger les systèmes informatiques et pour améliorer la planification d'urgence s'inscrivent dans une nouvelle prise de conscience, avec les années, du fait que la sécurité d'un pays ne dépend pas uniquement de sa capacité à se défendre contre des attaques militaires étrangères. Un pays qui ne serait pas bien équipé pour contrer la menace terroriste et pour atténuer les effets des grandes catastrophes naturelles pourrait connaître de graves bouleversements économiques et sociaux susceptibles de mettre sa sécurité en danger. Par conséquent, la protection de l'infrastructure essentielle demeurera sans doute une préoccupation majeure du gouvernement canadien pendant un certain temps encore, d'autant plus qu'il reste encore énormément de travail à faire pour établir une collaboration plus étroite entre les secteurs public et privé.